IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 28, No. 4, August, 2023, pp. 1019-1027
Journal homepage: http://iieta.org/journals/isi

A Naive Bayes-Driven Mechanism for Mitigating Packet-Dropping Attacks in Autonomous Wireless Networks

Desai Neela Megha Shyam[1*], Mohammed Ali Hussain[2]

[1] Department of Computer Science & Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram Guntur 522 302, India
[2] Department of Electronics and Computer Engineering, Koneru Lakshmaiah Education Foundation, Vaddeswaram Guntur 522 302, India

Corresponding Author Email: n.m.s.desai@hotmail.com

https://doi.org/10.18280/isi.280422

Received: 15 May 2023
Revised: 2 August 2023
Accepted: 16 August 2023
Available online: 31 August 2023

Keywords:
packet-dropping, malicious attacks, system faults, Intrusion Detection Systems (IDS), MANETs, and naive bayes

ABSTRACT

Autonomous wireless networks, characterized by peer-to-peer connectivity and dynamic topology, enable efficient internet access, irrespective of geographical constraints. Their applications span across disaster relief, military operations, road safety, and healthcare, areas where secure communication is indispensable. This paper addresses the crucial challenge of packet-dropping attacks in these networks, a security issue that has not yet been thoroughly explored in current literature. Conventional mechanisms for preventing packet-dropping often fail to differentiate between malicious attacks and system faults, underscoring the need for an effective classification system. Such a system should discern whether packet-dropping incidents are a result of malevolent attacks or system faults, and appropriately penalize only the malicious nodes. In this light, we introduce an Intrusion Detection System (IDS) based on the Naive Bayes algorithm to mitigate packet-dropping attacks in autonomous wireless networks. This algorithm has demonstrated efficacy in distinguishing between different categories based on statistical probabilities. By successfully mitigating both malicious attacks and system faults, our proposed IDS significantly enhances network performance. Simulation results confirm the effectiveness of the proposed IDS, showing notable improvements in packet delivery, delay, and energy efficiency. This IDS, therefore, not only detects and eliminates packet-dropping nodes that disrupt network operations but also extends the overall network performance.

1. INTRODUCTION

Wireless infrastructure-less networks, marked by autonomous and dynamic nodes, are often deployed in radio communication zones. Due to their inherent characteristics of autonomy, adaptability, and self-formation, these networks are particularly well-suited for applications where establishing infrastructure is both costly and time-consuming, such as healthcare, military, and disaster recovery [1].

The decentralized nature of these networks affords them flexibility, rapid deployment, and adaptability to varying environments. However, this lack of centralized control and established communication paths can result in increased packet loss. Given their free-roaming nature, nodes often change topology, and due to the dynamic nature of the network, route changes and disturbances can lead to packet loss. Furthermore, nodes are constrained by their limited processing power, energy (battery), memory, and bandwidth, which can lead to packet loss when data overload occurs. Wireless communication over long distances is susceptible to interference and signal attenuation, further contributing to packet loss. The voluntary nature of node participation in these networks can result in link failures when nodes join or leave the network. Without a central control unit to optimize and administer routing decisions, individual nodes rely on distributed algorithms, which can lead to packet loss in certain circumstances. Lastly, malicious nodes may intentionally discard packets to damage wireless ad-hoc networks, presenting a security barrier. System faults can also lead to packet loss on under-resourced nodes.

In these networks, applications demand secure connections. Communication is facilitated by determining the route between parties and transferring data along that path. However, due to the peer-to-peer nature of route computing, this process is both challenging and fragile. One major issue encountered during routing and data forwarding at the network layer is packet dropping by an intermediary node, either due to the node's malicious intent or system faults [2].

In wireless ad-hoc networks, direct communication between two nodes is possible when they are within each other's radio communication range, without the need for intermediaries or infrastructure. However, when the source and destination nodes are not within each other's radio communication range, a routing protocol may facilitate communication by leveraging intermediate nodes to establish a route between them [3]. This routing protocol operates under the assumption that intermediate nodes will cooperate and coordinate in the communication. However, this may not always be the case due to system faults or malicious behavior.

Packet dropping by an intermediate node due to malicious intent forms the basis for black hole attacks, wormhole attacks, and gray hole attacks, where packets are intentionally

discarded. Conversely, packets may unintentionally be dropped due to insufficient energy to process the packets, lack of space to hold the packets, or TTL time out [4]. This type of unintentional packet dropping is also referred to as system faults packet drop [5]. Thus, packet drops in the network can be categorized into two types: 1) Malicious packet drop, and 2) System fault packet drop. Packet loss in a network is a significant issue as it degrades network performance and disrupts application objectives by causing congestion and depleting network resources.

Various strategies proposed in the literature aim to exclude packet drop nodes from the communication stream. These techniques are primarily classified into three types: 1) Credit-based, 2) Monitoring-based, 3) Acknowledgment-based mechanisms. Credit-based systems allocate credits to nodes based on their behavior. Nodes then use these credits to participate in communication, with well-behaved nodes earning more credits. However, malicious nodes can exploit this system by behaving appropriately in non-malicious scenarios to earn credits, which they can then use to participate in communication. Monitoring-based techniques detect misbehaving activity by observing node behavior, traffic patterns, or performance indicators. Yet, real-time monitoring and analysis introduce overhead, and determining what constitutes malicious behavior in dynamic and distributed environments is a challenge. Acknowledgment-based techniques rely on node acknowledgments to confirm packet communication. In the event an intermediate node drops the packets, the sender will not receive an acknowledgment. These techniques handle general packet loss scenarios but do not distinguish between malicious and system fault packet loss.

Existing approaches fail to differentiate between packet drops caused by malicious attacks and system faults. Therefore, the aim of this paper is to design an intelligent Intrusion Detection System (IDS) capable of determining whether packet dropping is due to malicious intent or system faults.

2. LITERATURE REVIEW

The phenomenon of packet dropping, both intentional and unintentional, by intermediary nodes in a network pertains to the discarding of data packets. This occurrence is particularly noteworthy in Mobile Ad Hoc Networks (MANETs), where unintentional packet dropping can result from a variety of factors, including network congestion, a saturated buffer or energy constraints. The implications of packet dropping are far-reaching, leading to data loss, a decrease in network efficiency and an increase in latency. Furthermore, packet drops can represent a significant security threat, with severe consequences for the performance and reliability of the network.

Deliberate packet dropping, classified as malicious, involves the unlawful discarding of data packets by a rogue node. In a MANET, such malicious nodes can disrupt the routing process, leading to inefficient routing and hindering data from reaching its intended destination. This disruption diminishes the network's efficiency and dependability. Furthermore, by interfering with the network's ordinarily functioning protocol, malicious packet drops can expose security vulnerabilities, providing opportunities for exploitation by adversaries. An exemplary malicious packet dropping attack is the black hole attack, in which a rogue node falsely claims to possess the shortest path to the destination node, only to discard all received packets. This can culminate in a denial of service (DoS) attack.

Mitigation strategies for malicious packet drops in MANETs encompass various security measures. The implementation of robust security mechanisms can effectively minimize the risks associated with malicious packet drops, thereby ensuring the network's security and dependability. These measures span from authentication and encipherment to Trust-Based Approaches and Intrusion Detection Systems. Additionally, machine learning techniques can be employed to detect and respond to malicious nodes within the network.

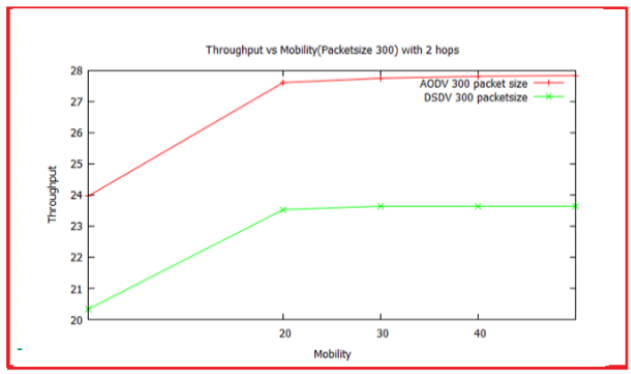

Figure 1. Throughput comparison of the MANETs with respect to reactive and proactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

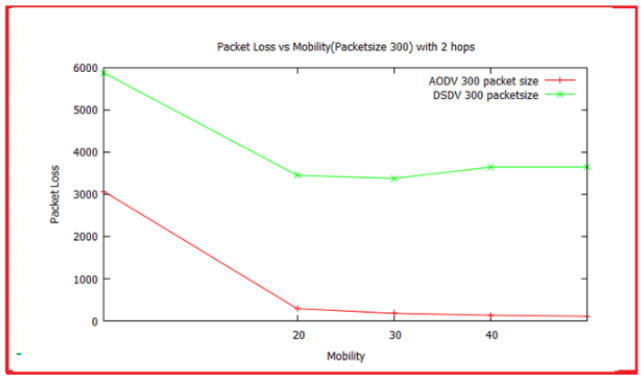

Figure 2. Packet loss comparison of the MANETs with respect to reactive and proactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

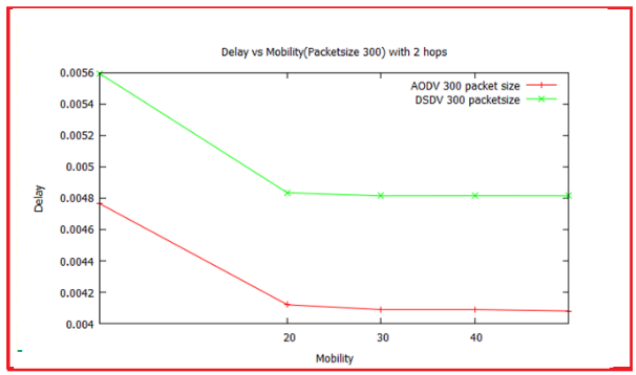

Figure 3. Delay comparison of the MANETs with respect to reactive and proactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

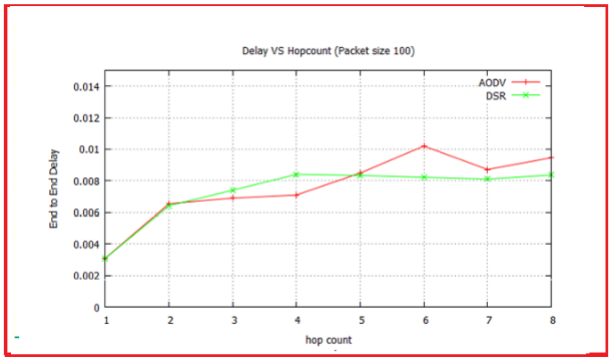

Figure 4. End to end delay comparison of the MANETs with respect to reactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

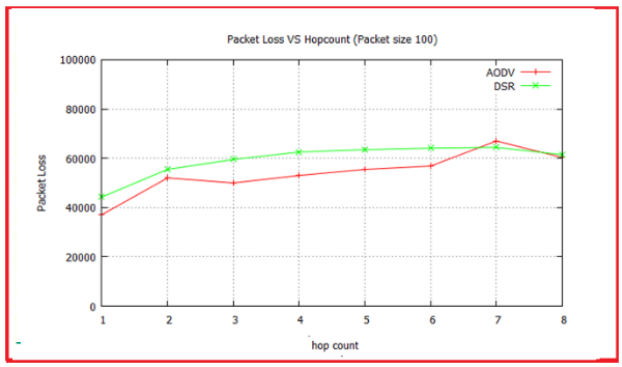

Figure 5. Packet loss comparison of the MANETs with respect to reactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

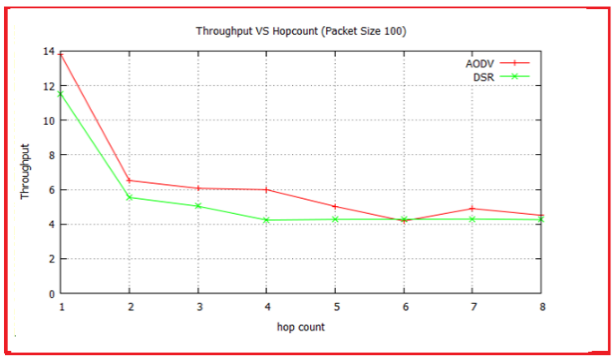

Figure 6. Throughput comparison of the MANETs with respect to reactive routing in the presence of the system fault packet dropping node with ACK based malicious node prevention mechanism

The literature presents a plethora of strategies aimed at precluding packet drop nodes from interfering with the communication stream. These techniques primarily fall into three categories: 1). Credit-based approaches [6-9], 2). Monitoring-based approaches [10-15], and 3). Acknowledgment-based mechanisms [16-18].

The credit-based techniques incentivize nodes to forward packets by providing them with credits that can be used to engage in communication. This system encourages nodes to act as intermediaries in the routing process, thereby indirectly promoting the forwarding of other nodes' packets. A notable example of a credit-based approach is CAODV [19], where nodes confer credits upon their neighboring nodes. Despite its effectiveness, this approach presents a challenge in wireless ad-hoc networks due to its reliance on a centralized approach, which is incompatible with the distributed nature of the network.

Monitoring-based packet dropping prevention techniques, also known as reputation-based techniques, operate by scrutinizing the behavior of nodes during packet processing. If a node is found to engage in malicious behavior, it is excluded from communication. However, continuous monitoring of nodes introduces overhead to the network.

Alternatively, acknowledgment-based techniques rely on the generation of an acknowledgment packet by the destination node in response to packet reception [3]. In the event that an intermediate node drops the packets, the sender will not receive an acknowledgment. These techniques demonstrate potential advantages over reputation-based and credit-based systems, offering lower overhead in memory and computation. However, their success is contingent on the validity and authenticity of the acknowledgment packets.

While the aforementioned categories are effective in detecting and preventing packet-dropping nodes from exiting the network, they fall short in distinguishing between intentional packet dropping attacks and system malfunctions. As a result, nodes that drop packets due to system faults are erroneously deemed malicious and removed from the communication path. This consideration exerts a profound impact on network performance, as demonstrated in Figures 1-6. We evaluated the performance of a MANET with an implemented Acknowledgement approach in terms of throughput, packet loss, and delay, in the presence of system fault packet dropping nodes.

The presence of system fault intermediate nodes in the communication path, despite the presence of a malicious packet prevention mechanism, significantly influences the performance of the network. Therefore, networks necessitate a packet drop prevention mechanism capable of identifying the cause of packet dropping and distinguishing between malicious packet dropping and packet dropping due to system faults. Furthermore, malicious packet-dropping nodes must be penalized. The aim of this study is to develop an intelligent intrusion detection technique capable of distinguishing between packet dropping caused by malicious attacks and system faults, and to penalize only the malicious nodes. To this end, a machine learning-based packet-dropping nodes classification mechanism is proposed, as the mitigation of malicious packet dropping is an anomaly mitigation-based problem where machine learning algorithms excel.

3. MACHINE LEARNING -BASED CLASSIFICATION MECHANISM

The detection of intrusions in MANETs is a critical objective, as it seeks to identify and counteract the harmful impact of nodes that are intentionally or unintentionally disrupting the regular functioning of the network. Machine learning algorithms have been increasingly used to address this challenge due to their ability to process large amounts of data and detect complex patterns. One of the ways in which machine learning can be used for intrusion detection in MANETs are; Classification: Machine learning algorithms

can be used to classify nodes based on their behaviour, such as normal or malicious, and take appropriate action based on these classifications. One such classification-based machine learning mechanisms used for intrusion detection in MANETs include Naive Bayes.

The Naive Bayes algorithm [20] is a machine learning technique that can be utilized to mitigate the risk of malicious packet dropping attacks in MANETs. The Bayes Theorem, on which the Naive Bayes algorithm is based, asserts that the likelihood of a hypothesis (H) given some evidence (E) is equal to the likelihood of the evidence given the hypothesis multiplied by the prior likelihood of the hypothesis. In the context of MANETs, the hypothesis is that a particular node is malicious, and the evidence consists of the network's behaviour and the characteristics of the node under scrutiny. When a node is classified as a malicious node, the algorithm can prevent it from participating in the network by either isolating it or routing around it. This helps to prevent the malicious packet dropping attacks, which is a form of denial-of-service attack that can cause the network to become congested and slow down. The work presents Naive Bayes-based Intrusion detection system (NB-IDS) which mitigates Packet-dropping attacks in Wireless infrastructure-less Networks.

The work uses a Naive Bayes-based intelligent Intrusion Detection System (IDS) to overcome packet dropping in wireless infrastructure-less networks. However, intentional packet dropping or system failures threaten network performance and security. Existing IDS fail to distinguish between intentional and fault-based packet drops, punishing both. For resource-constrained networks, the Naive Bayes method was chosen for its simplicity, efficiency, and data handling. The suggested IDS accurately classifies packet drops to identify hostile nodes and avoid penalising system errors, improving network speed and security.

To create a dataset for MANETs with malicious packet dropping nodes, unintentional packet dropping, and reputed nodes, we considered the following steps;

(1) Create a network of nodes: We used the NS2 simulator to create a MNAET, consists of 200 nodes, with 10 malicious packet dropping, and 10 unintentional packet dropping nodes network of nodes. The nodes are equipped with heterogeneous resources such as battery, buffer, and processor. The network consist of 10 sources and 10 destinations with multi hop communication. The route created between them using reactive and proactive routing protocols. Nodes mobile with the help of random way mobility model. Constant bit rate (CBR) application is used to create the traffic and it is attached with UDP protocol at transport layer for communication. The dataset will be prepared with the following information.

- The normal flow of the packet flow through the node
- Packet drop by nodes due to buffer overflow
- Packet drops by node due to lack of energy
- Packet drop by nodes due to TTL timeout
- Packet drop by nodes due to selfishness
- Packet drop by nodes due to malicious behavior

To malicious packet dropping attacks in MANETs, it is important to consider various network parameters or features. We consider features such as packet loss rate, average delay, routing information, node behavior, energy consumption, trustworthiness, number of hops, routing protocol used, node's mobility, network traffic volume, and traffic pattern to classify different types of nodes. NS2 simulator is run for 100 minutes and average of 10 times execution is used to collect the data.

The simulation setting was carefully made to reflect real-world problems in wireless networks with no infrastructure. Nodes were given 20-Joule batteries to simulate settings with limited resources, and they were set to move at a dynamic 20 m/s pause time to show that the network is always moving. With a radio range of 250 metres and 2 Mbps IEEE 802.11 MAC cards, nodes could talk to each other directly without going through a middleman. During data transfer, the power settings for receive and send activities (300mW and 600mW, respectively) also affected how much energy was used. A constant bit rate (CBR) programme made 512-byte packets to simulate how data traffic works in the real world. With these parameters, it is possible to get a good idea of how well the suggested Naive Bayes-based classification mechanism worked in real life.

Scenario-1: The Wireless infrastructure-less Networks network with 200 nodes with heterogeneous resources is constructed in the NS-2 simulator. The simulation environment was created so that multiple sources communicated with multiple destinations in a multi-hop manner without any packet drop. The complete information is collected and labelled as normal flow.

Scenario-2: In the same simulation environment, we made the constrained intermediate node in terms of a buffer to drop the packets during the communication. The complete information is collected and labeled as buffer overflow packet drop.

Scenario-3: Further, we made the constrained intermediate node in terms of energy to drop the packets during the communication. The complete information is collected and labeled as lack of energy packet drop.

Scenario-4: Further, we constructed a multi-hop communication environment, so that packet drops happen in the network due to the expiration of the packet lifetime. The complete information is collected and labeled as TTL timeout packet drop.

Scenario-5: Finally, we inserted the malicious packet-dropping node in the routing path to get packets dropped in the network. Here, we created malicious nodes as a blackhole and cooperative black hole nodes. The complete information is collected and labeled as malicious packet drops.

Finally, the dataset for Wireless infrastructure-less Networks (MANETs) is generated using the NS-2 simulator and five distinct scenarios. Scenario-1 establishes a normal communication flow between 200 nodes, with no packet loss; this serves as the baseline dataset. Scenario 2 entails constrained intermediate nodes dropping packets due to buffer overflow, whereas Scenario 3 simulates packet drops due to energy constraints in particular nodes. Scenario 4 generates a multi-hop environment in which TTL-expired packets are lost. Scenario 5 concludes with malicious nodes, including blackhole and cooperative black hole nodes, that lose packets on purpose. Each scenario's comprehensive information is compiled and appropriately labelled. This diverse dataset enables the evaluation of a proposed Naive Bayes-based Intrusion Detection System (IDS), which enhances security and efficiency in MANETs by distinguishing between normal and anomalous packet drops.

(2) Label data: Label the data based on the type of node it belongs to, such as malicious packet dropping node, unintentional packet dropping, and normal packet flowing nodes.

(3) Pre-process the data: The collected data is pre-processed to remove any irrelevant or missing values. The data is also

divided into two sets: a training set and a test set.

(4) Train the algorithm: The training set is used to train the Naive Bayes algorithm to identify normal network traffic patterns. The algorithm is trained to identify the relationship between different features of the network traffic data and to classify them as either normal or attack traffic.

(5) Testing the algorithm: The test set is then used to test the accuracy of the Naive Bayes algorithm. The algorithm is used to classify the network traffic data in the test set as either normal or attack traffic.

(6) During the data pre-processing stage of the Naive Bayes-based Intrusion Detection System (IDS) for MANETs, missing values are identified through data exploration and appropriate handling strategies, such as removing rows or imputing values, are implemented. On the basis of domain knowledge and feature importance techniques, irrelevant features are identified, and data normalisation or scaling is performed to bring the features to a common scale. The dataset is then typically divided into training and test sets at a ratio of 80-20 or 70-30. Using techniques such as oversampling, under sampling, and class-weighted algorithms, class imbalance is addressed. Feature engineering is used to create new features based on domain knowledge or mathematical operations performed on existing features. For efficient data pre-processing, Python libraries such as pandas, scikit-learn, and NumPy are frequently employed.

(7) Determine the threshold value: Based on the accuracy of the results, the threshold value is determined. This threshold value is used to differentiate between normal and attack traffic in the MANET. Our experiments environment opted the adjustable threshold value, as the adaptive technique outperformed the static threshold in classifying regular and malicious network traffic. The adaptive threshold was better at handling changing network circumstances. Thus, the adaptive threshold is better for our intrusion detection system because it performs better and adapts to changing network conditions.

(8) Monitor the network: The Naive Bayes algorithm is then used to monitor the network traffic in real-time. Any network traffic that exceeds the threshold value is classified as an attack, and appropriate action can be taken to prevent the black hole attack.

4. PERFORMANCE ANALYSIS

We tested how well our proposed Naive Bayes-based classification worked with the help of the NS2.34 simulator. In our simulation, we take into account a random waypoint mobility model with a 20 m/s pause time and a variable number of nodes. Each node starts out with a 20-joule battery, a 250-meter radio transmission range, and an IEEE 802.11 MAC card with a 2 Mbps data rate. The power to receive is 300 mW, and the power to send is 600 mW. Lastly, source nodes send CBR traffic that is 512 bytes in size. The simulation takes 1000 s, and we took the average of how well 3 different scenarios worked. In the simulation, three types of nodes are taken into account: I. Reputed nodes, which follow the routing protocol rules. II. Misbehaving nodes that drop packets on purpose because they are doing som ething bad. III. Misbehaving nodes that drop packets by accident because of buffer overflow or energy constraints. Here are the set threshold values for performance evaluation. Performance evaluation criteria for the proposed work include throughput, packet delivery percentage, overhead, and energy efficiency. These metrics give a full picture of how well the proposed Naive Bayes-based classification mechanism protects wireless infrastructure-less networks from packet-dropping attacks. They measure dependability, how well data is handled, how fast packets are sent, and how well resources are used.

A. Performance calculation scenarios

The primary purpose of this work is to explore the performance of the proposed Naive Bayes-based classification mechanism in a network with an intentional and unintended misbehaving node. As a result, we compare the proposed algorithm performance to that of two recently developed protocols, acknowledgment-based algorithm [4], secure knowledge algorithm [5] and both of which are designed to remove malicious nodes from the communication path. During performance evaluation, we assign the secure knowledge method SKA and the acknowledgment-based algorithm EAACK. We also evaluate the proposed routing protocol's performance to that of AODV-NM, a simple reactive routing system with no misbehaving nodes in the network. ERMMN is a Naive Bayes-based classification method that has been proposed.

The performance is assessed by taking into account the simulated scenario below.

(1) The network is made up of unintentional and purposeful packet dropping nodes, as well as respected nodes. Unintentionally misbehaving nodes drop the packet due to either buffer overflow or energy constraint, or both. The maliciously misbehaving nodes delete all packets received and transmit a bogus report to the source. The goal of this scenario is to assess existing system weaknesses as well as how performance is expanded in the proposed work. The goal of this scenario is to put the proposed changes to the test against intentionally misbehaving nodes. The performance evaluation is then calculated using the three conditions listed below.

(2) The variable number of nodes involved in multiple-hop communication between communication entities.

(3) Vary the number of nodes during the simulation

B. Performance results

The effectiveness of the Naive Bayes algorithm in detecting and classifying network traffic as either normal or attack traffic will be evaluated. To assess its efficacy, we will employ a variety of metrics, including packet delivery fraction, throughput, end-to-end delay, and energy efficiency. The packet delivery fraction measures the percentage of successfully delivered packets, whereas the throughput indicates the quantity of data transmitted over the network in a given amount of time. End-to-end delay will evaluate the amount of time it takes for a packet to reach its destination, while energy efficiency will assess the network's energy consumption. By comparing the performance of the Naive Bayes algorithm to that of extant intrusion detection techniques, we hope to demonstrate its superiority in detecting and mitigating malicious traffic while minimising false positives and negatives.

Both proposed and existing routing protocols are assessed and compared in an identical network environment to evaluate their respective performances. The following describes the simulation findings in several network environments with different performance calculation measures.

C. Packet delivery fraction

The packet delivery fraction is measured and contrasted against varying node counts in the presence of both deliberate and unintentional misbehaving nodes. This enables a comprehensive evaluation of the network's performance under

diverse scenarios. The EAACK [5] protocol performs badly because no mechanism exists to deal with inadvertently misbehaving nodes. SKA [4] outperforms EAACK because it analyses the causes of packet drops after identifying the offender node.

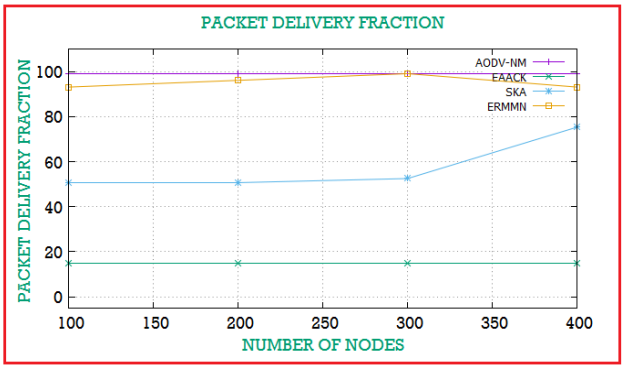

Figure 7. Performance evaluation in terms of packet delivery fraction

Figure 7 depicts the performance of the packet delivery fraction of existing and proposed Naive Bayes-based mechanism when the number of nodes is varied. Under no misbehaving nodes conditions, the proposed Naive Bayes-based classification mechanism packet delivery percentage is nearly similar to reactive routing protocol. The EAACK protocol performs poorly since this strategy did not account for unintended packet drop nodes mitigation.

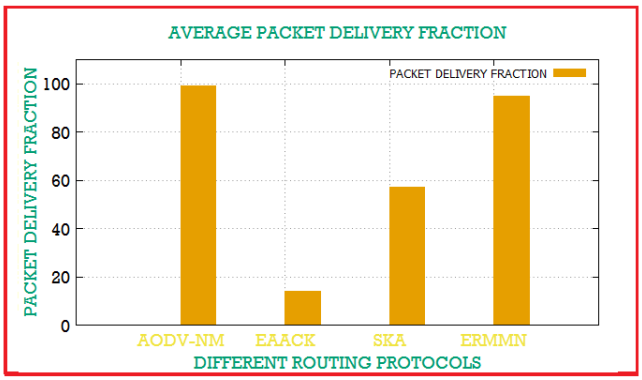

Figure 8. Performance comparison in terms of packet delivery fraction for proposed and existing approaches

Figure 8 depicts the average packet delivery fraction of existing and proposed Naive Bayes-based mechanism for a given number of nodes. Under no misbehaving nodes conditions, the Naive Bayes-based mechanism's average packet delivery fraction is nearly equivalent to that of the reactive routing protocol. The acknowledgement-based technique performs poorly because it does not account for purposeful misbehaving node prevention. Figures 8 and 9 show that the proposed Naive Bayes-based mechanism outperforms existing techniques. The suggested protocol nearly reaches the value of reactive routing protocol performance under no misbehaving node scenario. The proposed Naive Bayes-based mechanism outperforms existing techniques in terms of performance since it removes both unintentional and intentional packet drops from the communication.

Proposed Naive Bayes-based classification mechanism has a high packet delivery rate shows that it works well to keep data transmission reliable in wireless networks without infrastructure. Because the work can tell the difference between malicious and accidentally misbehaving nodes, it can stop malicious nodes from stopping communication by taking the right steps. As a result, the network drops fewer packets, which means a higher percentage of packets are delivered. This finding matches the main goal of the study, which was to stop packet-dropping attacks and make sure communication is reliable.

D. Throughput

To estimate the network throughput under different scenarios, a variable number of nodes and simulation duration are employed, with both deliberate and unintentional misbehaving nodes included. However, due to limited resources and the inability to prevent packet dropping nodes from the routing path, the performance of the EAACK [5] protocol is significantly impacted, resulting in low network throughput.

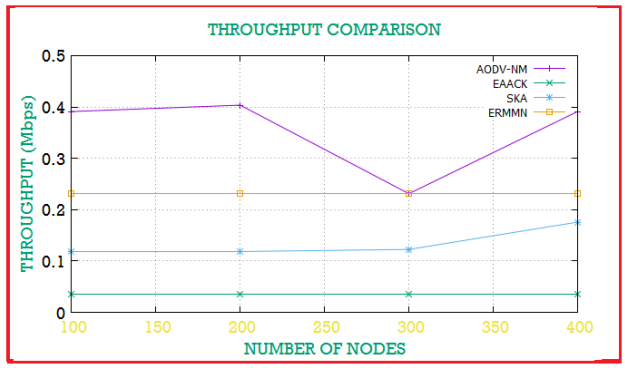

Figure 9. Performance evaluation in terms of throughput (Mbps)

In Figure 9, a comparison of the throughput performance of the proposed Naive Bayes-based mechanism with existing routing protocols is presented as a function of the number of nodes in the network. The Naive Bayes-based method outperforms the EAACK and SKA algorithms in terms of throughput performance, as it can prevent packet drops caused by limited resources.

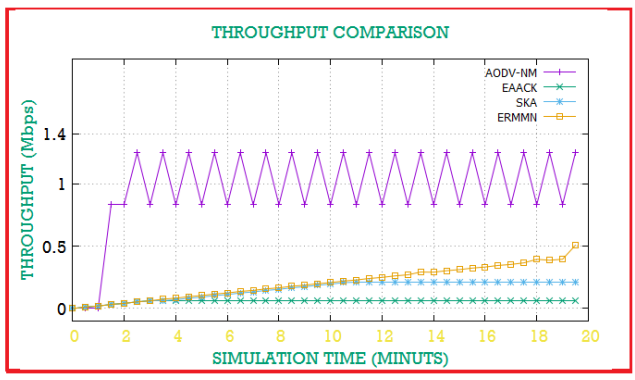

Figure 10. Performance comparison in terms of throughput (Mbps) for proposed and existing approaches

Figure 10 compares the simulation time throughput performance of the proposed Naive Bayes-based method and existing routing protocols. The proposed Naive Bayes-based method throughput outperforms the EAACK and SKA

algorithms because it prevents packet drops due to limited resources. Figure 11 compares the average throughput performance of the proposed Naive Bayes-based mechanism and existing routing protocols over a range of node counts. The proposed Naive Bayes-based mechanisms have a higher average throughput than the EAACK and SKA algorithms because they prevent packets from dropping due to limited resources.

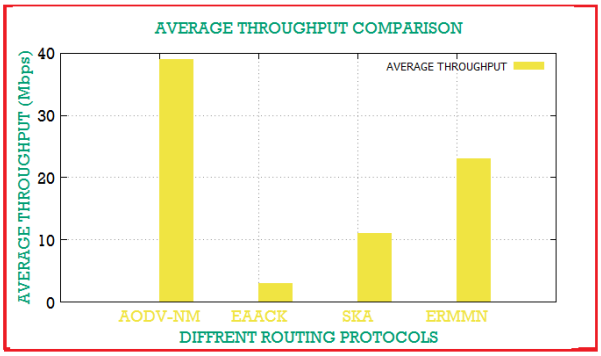

Figure 11. Performance comparison in terms of average throughput (Mbps)

Figures 9-11 show that the proposed Naive Bayes-based method outperforms the previous approaches. The proposed mechanism performance nearly equals the value of reactive routing protocol performance under no misbehaving node situation. The proposed Naive Bayes-based solution outperforms existing approaches because it avoids unintended packet dropping nodes and mitigates intentional misbehaving nodes from the routing path.

Proposed algorithm's better throughput can be explained by how well it deals with nodes that don't behave as expected. By correctly classifying nodes and isolating bad ones, the work keeps the network from getting clogged up and makes sure that data flows more smoothly. Keeping packets from being dropped on purpose or by accident helps improve data handling speed and increase throughput. This finding fits with the goal of the study, which was to improve the network's performance a lot by getting rid of disruptive packet-dropping nodes.

E. End-to-end delay

By adjusting the number of nodes and simulation time when deliberate and inadvertent misbehaving nodes are present, the network's end-to-end delay is calculated. The designed Naive Bayes-based method has a lower delay than EAACK but a higher delay than the SKA approach. Because the SKA system lacked an authentication mechanism and a digested acknowledgment mechanism, it did not reduce false misbehaving nodes. As a result, SKA has a lower latency than EAACK and the proposed Bayes-based method, ERMMN.

Figure 12 shows a comparison of the end-to-end delay performance of the proposed protocol and existing protocols with a varying number of nodes. The results indicate that the proposed protocol outperforms the EAACK protocol in terms of end-to-end delay, thus demonstrating its effectiveness in mitigating malicious attacks and improving the overall network performance.

Figure 13 compares the end-to-end delay performance of proposed and current protocols in terms of simulation time. The proposed protocol latency is greater early in the simulation time, but afterwards it is about the same as other alternatives.

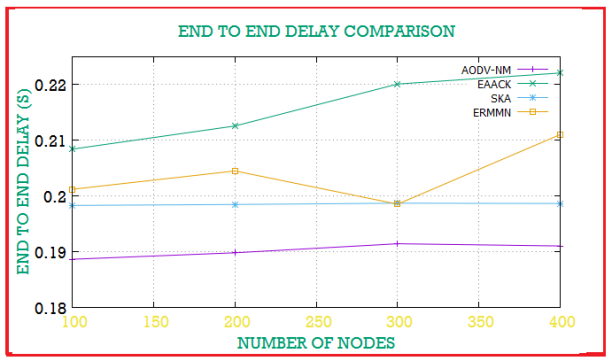

Figure 12. Performance comparison in terms of end-o-end delay (s)

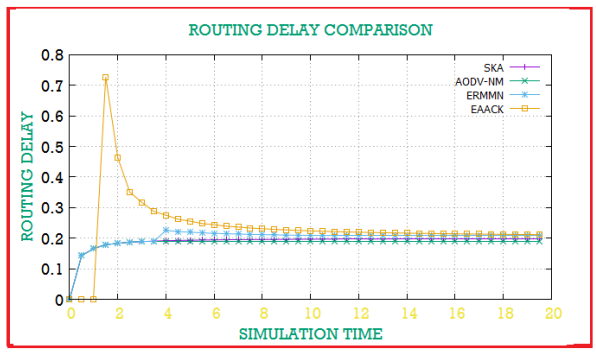

Figure 13. Performance comparison in terms of end-to-end delay (s) with respect to simulation time

The proposed algorithm has a lower end-to-end delay, which means that data is sent faster and there is less latency in the network. By quickly figuring out which nodes are bad and isolating them, the work optimises the routing paths and cuts down on the delays caused by disruptions. Also, preventing packets from being dropped by accident because of a lack of resources helps reduce end-to-end delays. This finding fits with the study's goal of reducing packet-dropping attacks to improve network efficiency and application performance.

F. Energy efficiency

The network's energy consumption is calculated in relation to the number of nodes and is also compared to the network's packet delivery fraction and throughput.

Figure 14 compares the leftover energy of a network of planned and current protocols with a changing number of nodes. The proposed protocol network conserves energy by taking the energy efficiency metric into account during the routing process. Existing protocols have less remaining energy since energy economy is not considered during the routing phase.

Figure 15 depicts a comparison of the network's residual energy with respect to the packet delivery percentage of proposed and current protocols in an equivalent network context. All other approaches are outperformed by the proposed protocol's packet delivery fraction and residual energy performance.

Figure 16 compares the network's residual energy to the throughput of proposed and existing protocols in an equivalent network configuration. The proposed protocol outperforms the conventional ACK-based technique. This is because the suggested protocol reduces packet drops in a network, improving energy efficiency.

The reason the proposed algorithm uses less energy is

because it stops malicious nodes from using up network resources and draining the energy of nearby nodes. The work saves energy and extends the life of the network by correctly classifying nodes and removing malicious ones from the communication path. The goal of the study was to find the best way to use resources and save energy in wireless networks without infrastructure.

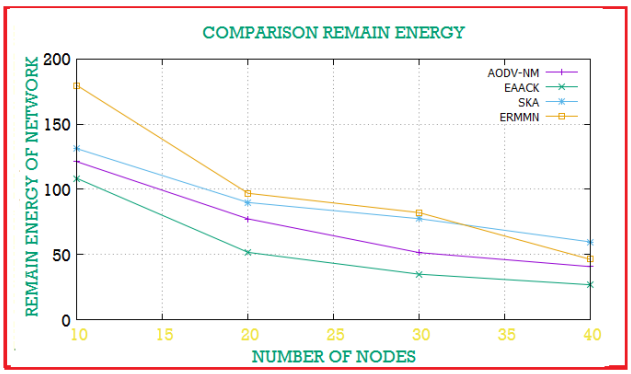

Figure 14. Performance comparison in terms of average reaming energy of nodes

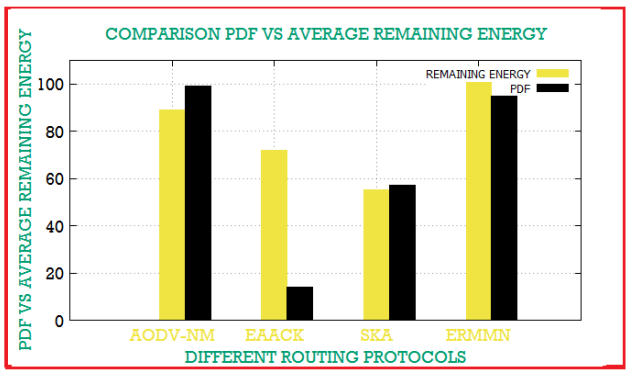

Figure 15. PDF vs Average reaming energy comparison

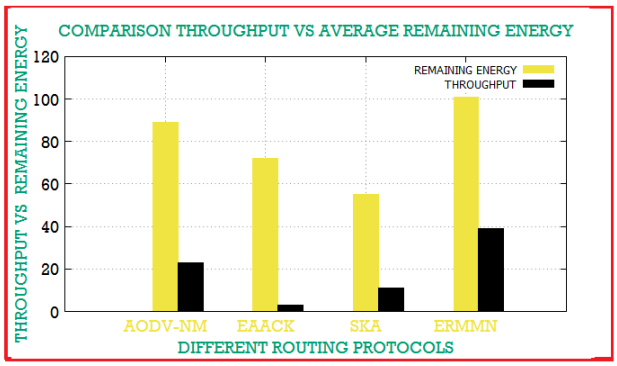

Figure 16. Throughput (Mbps) vs Average remaining energy comparison

The comparison shows that the suggested Naive Bayes-based classification mechanism is better than existing protocols at dealing with problems caused by nodes that act badly on purpose or by accident. The suggested algorithm improves the performance and security of wireless networks without infrastructure by allowing for accurate classification and strong intrusion detection.

The results of our study show that the Naive Bayes-based classification method is a good way to improve the security and reliability of wireless networks without infrastructure. By correctly identifying malicious and unintentionally misbehaving nodes, the algorithm makes sure that data is sent quickly and resources are used well. This makes it a strong way to stop packet-dropping attacks in the real world.

The performance analysis shows that the proposed Naive Bayes-based classification mechanism is better than current protocols at stopping packet-dropping attacks and making wireless networks that don't have any infrastructure work better. The algorithm can correctly tell the difference between malicious and unintentionally misbehaving nodes. This lets it take targeted actions that improve packet delivery, throughput, end-to-end delay, and energy efficiency. The suggested algorithm makes the best use of resources, cuts down on communication delays, and extends the life of networks by handling both intentional and unintentional packet drops well. These results show how important the suggested method is in the real world for achieving the study's goals of securing network communication and making networks more reliable and efficient.

5. CONCLUSION

Wireless infrastructure-less Networks is an autonomous, peer-to-peer, and dynamic topological networks. It enables internet connectivity, regardless of geographical location, effectively in terms of cost and time. The applications of the networks are disaster relief, military, road safety, and healthcare. The applications are susceptible and demand secure communication. The paper aims to mitigate packet-dropping attacks and demonstrates that conventional packet-drop-preventing mechanisms fail to differentiate malicious attacks and system faults. Thus, there is a requirement for a proper packet-dropping nodes classification mechanism that must identify whether packet-dropping is actually due to malicious attacks or system faults. Further, it only punishes the malicious nodes. The work presented Naive Bayes -based classification mechanism which mitigates Packet-dropping attacks in Wireless infrastructure-less Networks. The proposed algorithm is able to tell the difference between malicious and accidentally misbehaving nodes, which greatly improves the performance of the network. Extensive simulations show that it is better than current protocols, with higher packet delivery, better throughput, less delay from end to end, and better use of energy. The practical value of the algorithm is shown by the fact that it could be used in disaster relief, military activities, and healthcare networks. In the future, study could focus on improving the accuracy of the mechanism, making it work against other types of attacks, and testing how well it can adapt to different dynamic network environments. Overall, this work is a useful contribution to wireless network security, opening the door to new ideas and developments in this field.

REFERENCES

[1] Ramphull, D., Mungur, A., Armoogum, S., Pudaruth, S. (2021). A review of mobile ad hoc NETwork (MANET) Protocols and their Applications. In 2021 5th international conference on intelligent computing and control systems (ICICCS), Madurai, India, pp. 204-211. https://doi.org/10.1109/ICICCS51141.2021.9432258

[2] Siddiqua, A., Sridevi, K., Mohammed, A.A.K. (2015). Preventing black hole attacks in MANETs using secure knowledge algorithm. In 2015 International Conference on Signal Processing and Communication Engineering Systems, Guntur, India, pp. 421-425. https://doi.org/10.1109/SPACES.2015.7058298

[3] Mohammad, A.A.K., Mahmood, A.M., Vemuru, S. (2019). Intentional and unintentional misbehaving node detection and prevention in mobile ad hoc network. International Journal of Hybrid Intelligence, 1(2-3): 239-267. https://doi.org/10.1504/IJHI.2019.103580

[4] Zahid, S., Ullah, K., Waheed, A., Basar, S., Zareei, M., Biswal, R.R. (2022). Fault tolerant DHT-based routing in MANET. Sensors, 22(11): 4280. https://doi.org/10.3390/s22114280

[5] Shakshuki, E.M., Kang, N., Sheltami, T.R. (2012). EAACK-a secure intrusion-detection system for MANETs. IEEE Transactions on Industrial Electronics, 60(3): 1089-1098. https://doi.org/10.1109/TIE.2012.2196010

[6] Bansal, A., Varshney, A., Matta, R., Khanna, A. (2016). Acknowledgement based approaches for detecting routing misbehaviour in MANETs. In 2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, pp. 835-840.

[7] Mohamed, M.A., Mostafa, H.S., Eissa, M.E. (2016). Novel evaluation of ACK based IDS techniques for dropping attack in MANETs using OMNET++ simulator. International Journal of Computer Applications, 150(6).

[8] Deepa, M., Parvathi, M. (2015). Adoption of hybrid cryptography in an acknowledgement-based intrusion detection system for Manets. International Journal, 4(4): 79-82.

[9] Liu, K., Deng, J., Varshney, P.K., Balakrishnan, K. (2007). An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5): 536-550. https://doi.org/10.1109/TMC.2007.1036

[10] Shah, R., Subramaniam, S., Lekala Dasarathan, D.B. (2016). Mitigating malicious attacks using trust based secure-before routing strategy in mobile ad hoc networks. Journal of Computing and Information Technology, 24(3): 237-252. https://doi.org/10.20532/cit.2016.1002835

[11] Shah, S.N., Jhaveri, R.H. (2016). A trust-based scheme against Packet dropping attacks in MANETs. In 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT), Bangalore, India, pp. 68-75. https://doi.org/10.1109/ICATCCT.2016.7911967

[12] Wei, D., Cao, H., Liu, Z. (2016). Trust-based ad hoc on-demand multipath distance vector routing in MANETs. In 2016 16th international symposium on communications and information technologies (ISCIT), Qingdao, China, pp. 210-215. https://doi.org/10.1109/ISCIT.2016.7751623

[13] Jawhar, I., Mohammed, F., Al Jaroodi, J., Mohamed, N. (2016). TRAS: A trust-based routing protocol for ad hoc and sensor networks. In 2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity), New York, NY, USA, pp. 382-387. https://doi.org/10.1109/BigDataSecurity-HPSC-IDS.2016.58

[14] Bhalaji, N., Selvaraj, C. (2017). Comprehensive trust based scheme to combat malicious nodes in MANET based cyber physical systems. In Proceedings of International Conference on Communication and Networks: ComNet 2016, pp. 543-550. https://doi.org/10.1007/978-981-10-2750-5_56

[15] Tan, S., Li, X., Dong, Q. (2015). Trust based routing mechanism for securing OSLR-based MANET. Ad Hoc Networks, 30: 84-98. https://doi.org/10.1016/j.adhoc.2015.03.004

[16] Janzadeh, H., Fayazbakhsh, K., Dehghan, M., Fallah, M.S. (2009). A secure credit-based cooperation stimulating mechanism for MANETs using hash chains. Future Generation Computer Systems, 25(8): 926-934. https://doi.org/10.1016/j.future.2008.12.002

[17] Hubaux, J.P., Gross, T., Le Boudec, J.Y., Vetterli, M. (2001). Toward self-organized mobile ad hoc networks: The Terminodes Project. IEEE Communications Magazine, 39(1): 118-124. https://doi.org/10.1109/35.894385

[18] Jakobsson, M., Hubaux, J.P., Buttyán, L. (2003). A micro-payment scheme encouraging collaboration in multi-hop cellular networks. In Financial Cryptography: 7th International Conference, FC 2003, Guadeloupe, French West Indies, pp. 15-33. https://doi.org/10.1007/978-3-540-45126-6_2

[19] Saetang, W., Charoenpanyasak, S. (2012). Caodv free blackhole attack in ad hoc networks. In International Conference on Computer Networks and Communication Systems (CNCS 2012) IPCSIT, 35: 63-67.

[20] Berrar, D. (2018). Bayes' theorem and naive Bayes classifier. Encyclopedia of bioinformatics and computational biology: ABC of bioinformatics, 403: 412.